Розробка наукових засад побудови джерел живлення мікроконтролерів для створення нової технології захисту інформації в комп'ютерних системах.
Разработка научных основ построения источников питания микроконтроллеров для создания новой технологии защиты информации в компьютерных системах.
Elaboration of scientific fundamentals of building of microcontroller power sources for creation of the new technology of information protection in computer systems.

1. **Номер державної реєстрації** - 109U002766
2. **Науковий керівник** - д.т.н., проф. Терещенко Тетяна Олександрівна, Терещенко Татьяна Александровна, Tereschenko Tatyana.
3. **Суть розробки, основні результати**

(укр.)

В результаті проведення роботи виконано порівняльний аналіз існуючих систем захисту мікропроцесорних систем з метою виявлення їх недоліків та перспектив до покращення. Досліджено існуючі мікроконтролери на предмет захищеності від зчитування за струмом споживання, визначено реальну захищеність сучасних мікроконтролерів та запропонувано шляхи для збільшення їх захищеності. Розвинено алгоритм дискретного вейвлет-аналізу та спектрального аналізу в полярних координатах. Запропоновано нове вейвлет-перетворення в полярних координатах;, Розроблено нові способи та пристрої захисту інформації в мікроконтролерах від недеструктивних атак шляхом модифікації струму споживання. Створено алгоритми роботи джерел живлення із захистом за струмом споживання. зокрема алгоритми обчислення інтегрального коефіцієнту в полярних координатах для ідентифікації команд у реальному масштабі часу, та програмне забезпечення визначення рівня захищеності пам'яті програм мікроконтролерів; нові методи і алгоритми вейвлет-аналізу із заданим числом високочастотних фільтрів для дослідження струмів споживання мікроконтролера; формування бази даних часових залежностей струмів споживання для кожної інструкції мікроконтролера та їх спектрів у різних базисах.. Досліджено ефективність роботи запропонованих у роботі джерел живлення мікроконтролерів, розроблених алгоритмів та пристроїв. Результати роботи будуть використані для створення комп'ютерних та мікропроцесорних систем, захищених від несанкціонованого доступу. Можливими користувачами є підприємства та науково-дослідні організації, які займаються розробкою пристроїв мікропроцесорної техніки та мікропроцесорних систем керування із захистом інформації. Розроблені теоретичні засади та системи є перспективними для захисту конфіденційної інформації від несанкціонованого доступу у інформаційних системах безпеки, секретного документообігу, платіжних картках, картках електронного підпису та аутентифікації користувача при віддаленому доступі до корпоративних мереж.

(рос.)

В результате выполнения работы проведен сравнительный анализ существующих систем защиты микропроцессорных систем с целью выявления их недостатков и перспектив улучшения. Исследованы существующие микроконтроллеры на предмет защищенности от считывания по току потребления, определена реальная защищенность современных микроконтроллеров и предложены пути ее повышения. Получил дальнейшее развитие алгоритм дискретного вейвлет-анализа и спектрального анализа в полярных координатах. Предложено новое вейвлет-преобразование в полярных координатах; разработаны новые способы и устройства защиты информации в микроконтроллерах от недеструктивных атак путем модификации тока потребления. Созданы алгоритмы работы источников питания с защитой по току потребления, в частности, алгоритмы вычисления интегрального коэффициента в полярных координатах для идентификации команд в реальном масштабе времени, программное обеспечение определения уровня защищенности памяти программ микроконтроллеров; новые методы и алгоритмы вейвлет-анализа с заданным числом высокочастотных фильтров для исследования токов потребления микроконтроллера;

сфрмированы базы данных временных зависимостей токов потребления для каждой инструкции микроконтроллера и их спектры в различных базисах. Исследована эффективность работи предложенных в работе источников питания микроконтроллеров, разработанных алгоритмов и устройств. Результаты работы будут использованы для создания компьютерных и микропроцессорных систем, защищенных от несанкционированного доступа. Возможными пользователями являются предприятия и научно-исследовательские организации, которые занимаются разработкой устройств микропроцессорной техники и микропроцессорных систем управления с защитой информации.

(англ.)

As the result of research work a comparative analysis of existing security systems of microprocessor-based systems was made with aim to identify their disadvantages and improvement prospects. Existing microcontrollers were explore with aim to protection from readers on current consumption are researched and to determine the real security of high end microcontrollers and suggest ways to improve it. The algorithm of discrete wavelet analysis and spectral analysis in polar coordinates was further developed. A new wavelet transform in polar coordinates is offered. The new methods and devices of information protection in microcontrollers from non-destructive attacks by modifying the current consumption are developed. Algorithms of work of power supplies with protection on a consumption current, in particular, algorithms of computing of integrated factor in polar coordinates for identification of commands in real time, the software of definition level of security memory programs of microcontrollers are development; the new methods and algorithms of the wavelet -analysis with the set number of high-frequency filters to research the current consumption of the microcontroller; the databases of time dependences of current consumption for each instruction of the microcontroller and their spectrums in various bases are generated. Overall performance of the power supplies of the microcontrollers and developed algorithms and devices is researched in work. The results of work will be used for development of the computer and microp

4. **Наявність охоронних документів на об’єкти права інтелектуальної власності** (заявка на патент, патент, свідоцтво на авторське право).
    1. Патент №43673, G06K 19/06. Мікропроцесорна система із захистом інформації від зчитування за струмом споживання / Беженар В.О., Мороз А.В., Терещенко Т.О. (Україна). - Дата публікації 25.08.2009 р., бюл. №16;
    2. Патент №43673, G06F 1/00. Мікроконтролер з системою захисту від атак за струмом споживання / Беженар В.О., Мороз А.В., Терещенко Т.О. (Україна). - Дата публікації 25.08.2009 р., бюл. №16.
    3. Марчук Д.О., Колотов М.В., Петергеря Ю.С. Свідоцтво про реєстрацію авторського права на твір № 30094 Комп'ютерна програма “Прогнозування значень дискретних функцій з використанням нейронної мережі та вейвлет-перетворень ”, зареєстровано 11.02.2009 р., заявник — НТУУ “КПІ”.
5. **Порівняння зі світовими аналогами.**

Розроблені теоретичні засади та системи є перспективним для захисту конфіденційної інформації від несанкціонованого доступу у інформаційних системах безпеки, секретного документообігу, платіжних картках, картках електронного підпису та аутентифікації користувача при віддаленому доступі до корпоративних мереж. Науково-технічний рівень розробки відповідає кращим вітчизняним та зарубіжним аналогам світового рівня.

6. **Економічна привабливість для просування на ринок (вартість реалізації проекту, терміни впровадження та окупності, показники**).

Розроблені системи захисту на базі ключів та резисторів, що перемикаються, та на базі конденсаторів дозволяють за тієї ж вартості аналогів отримати більшу функціональність та рівень захисту завдяки застосуванню програмного генератора випадкових чисел. Системи захисту на базі двоядерних процесорів дозволяють забезпечити високий ступінь захищеності інформації від зчитування та несанкціонованих атак і мають на 12% меншу собівартість в

порівнянні з існуючими системами, які мають аналогічний ступінь захисту. Зменшення кількості вейвлет-коефіцієнтів у алгоритмі аналізу даних призводить до кращого стиснення інформації, що дозволяє спростити реалізацію систем, збільшити швидкість передачі даних по каналу зв'язку. Таким чином, розроблена науково-технічна продукція - фундаментальні засади побудови систем захисту мікроконтролерів - має економічну привабливість для просування на ринок сучасних наукоємних технологій захисту інформації, впровадження та реалізації у системах безпеки даних за рахунок зменшення собівартості при розширеній функціональності.

7. Потенційні користувачі (галузі, міністерства, відомства, підприємства, організації).

Використання результатів наукових досліджень при створенні нових систем захисту інформації у мікроконтролерах для систем керування вентильних перетворювачів в Інституті електродинаміки НАН України, Національному технічному університеті «Харківський політехнічний інститут» (м. Харків), Національному університеті кораблебудування ім. Адмірала Макарова (м. Миколаїв). ВО "Радіовимірювач", НПО "Сатурн"\Міністерство внутрішніх справ, Служба безпеки України, Національний банк України, ТОВ "Ulys Systems"

8. Стан готовності розробки (лабораторний або промисловий зразок, технічна документація, бізнес-план, готова до впровадження).

9. Існуючі результати впровадження.

Розроблений та виготовлений макет тестової плати для порівняння запропонованих і декількох типових систем захисту. Розроблено програмне забезпечення оцінки ступеню захищеності даних та програм у мікроконтролері. Можлива розробка дослідно-промислових зразків систем захисту на базі двоядерного процесора, які можуть бути впроваджені у промислове виробництво

10. Назва підрозділу, телефон, e-mail.

Науково-дослідний інститут прикладної електроніки Національного технічного університету України "КПІ", (044) 236-96-76, e-mail: bogdan@ee.ntu-kpi.kiev.ua

11. Перелік публікацій за матеріалами досліджень за період виконання: (монографії, підручники, посібники, наукові статті, дисертації, інші публікації).

Підручники:

1. Терещенко Т.О. Мікропроцесори та мікроконтролери / Т.О Терещенко, В.Я. Жуйков, Ю.В. Хохлов та ін. // Електронний підручник з грифом МОНУ www.kaf-pe.kpi.ua Гриф надано Міністерством освіти і науки України (лист № 1.4_18-Г-114 від 10.01.2009 р. - Тип носія - сервер веб-сайту, фізичний формат запису - .zip Windows - 557 с.
2. Бойко В.І. Цифрова схемотехніка електронних систем / В.І. Бойко, А.М. Гуржій, В.Я. Жуйков , Т.О. Терещенко та ін. // К.: Вища школа, 2010 (лист МОНУ № 1.4/18-Г-848 від 10.01.2008 р.) - 420 с.
3. Бойко В.І. Аналогова схемотехніка та імпульсні пристрої / В.І Бойко, А.М. Гуржій, В.М. Співак, Т.О. Терещенко та ін. // К.: Освіта України, 2010 (лист МОНУ № 1.4/18-Г-1656 від 07.07.2008 р) – 420 с.

Навчальні посібники:

1. Дискретные спектральные преобразования на конечных интервалах: учеб. пособие / В.Я. Жуйков, Т.А. Терещенко, Ю.С. Петергеря. – К.: НТУУ «КПІ», 2010. – 244 с.
2. Передача сигналов управления в условиях помех: учеб. пособие / В.Я. Жуйков, Т.А. Терещенко, Ю.В. Хохлов. – К.: НТУУ «КПІ», 2010. – 220 с. ,– Библиогр.: с.172-180. – 200 экз.

Наукові статті:

1. **Беженар В.О (студент).** Захист інформації від зчитування за струмом споживання з використанням генератора випадкових чисел / В.О. Беженар, А.В. Мороз, Т.О. Терещенко // Технічна електродинаміка. Темат. вип. „Силова електроніка та енергоефективність”. – Ч. 1. – 2009. – С. 39-42.

2. Терещенко Т.А. Применение дискретных спектральных преобразований во вращающихся координатах для дистанционного управления преобразователями / Т.А. Терещенко, Ю.В. Хохлов, Д.В. Лазарев // Технічна електродинаміка. Темат. вип. „Силова електроніка та енергоефективність”. - Ч.1. – 2010. – С.209-210.
3. Терещенко Т.А. Ориентированные спектральные преобразования в задачах управления, передачи сигналов и диагностики / Т.А. Терещенко, Ю.С. Петергеря, Ю.В. Хохлов // Технічна електродинаміка. Темат. вип. „Силова електроніка та енергоефективність”. - Ч.2. – 2010. – С.104-109.
4. Терещенко Т.О. Способи синхронізації в системах дистанційного керування перетворювачами / Т.О. Терещенко, Д.В.Лазарєв // Технічна електродинаміка. Темат. вип. “Проблеми сучасної електротехніки”. - Ч.1. – 2010. – С.63-66.
5. Терещенко Т.О. Швидкий алгоритм синхронізації в системах зв’язку з розширенням спектру / Т.О.Терещенко, Д.В.Лазарєв // Електроніка та зв’язок. Темат. вип. “Електроніка та нанотехнології”. - № 3 (56). – 2010. – С.190-193.
6. Беженар В.О. Цифрова система захисту від атак за струмом споживання / В.О. Беженар, А.В. Мороз, Т.О. Терещенко // Електроніка та зв’язок. Темат. вип. “Електроніка та нанотехнології”. - №.2 (55). – 2010. – С.108-114.
7. Лесовая М.А. Моделирование системы электропитания с резервными источниками / М.А. Лесовая, Е.С. Пичкалёв, Т.А. Терещенко, Ю.В. Хохлов // Електроніка та зв’язок. Темат. вип. “Електроніка та нанотехнології”, ч.4. – 2010. – С.91-95.
8. Петергеря Ю.С. Широтно-импульсные преобразователи постоянного напряжения в системе электропитания с солнечной батареей / Ю.С. Петергеря, Е.С. Пичкалев, Т.А. Терещенко, А.Л. Осадчий // Технічна електродинаміка. Темат. вип. “Проблеми сучасної електротехніки”, ч.1. – 2010. – С.116-119. URL
9. Петергеря Ю.С Модель процесса принятия решений при управлении электропотреблением \ Ю.С. Петергеря., А.Г. Киселёва // Збірник статей конференції «Моделювання-2010» . -Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, г. Киев. – С.230-237.
10. Петергеря Ю.С. Построение логического вывода в контекстно-зависимой системе управления электропотреблением / Ю.С. Петергеря, А.Г. Киселёва // Материалы десятой международной конференции «Интеллектуальный анализ информации» / Министерство образования и науки Украины, НТУУ «КПИ». — К.: НТУУ «КПИ», 2010.
11. Петергеря Ю.С. Теорія та засоби побудови енергоефективних систем керування електроживленням локальних об’єктів / Ю.С. Петергеря, Т.А. Хижняк, І.В. Блінов, В.В. Чопик // Технічна електродинаміка. – Тематичний випуск „Проблеми сучасної електротехніки”. - 2010. – Ч.1 – С.43-48.
12. Петергеря Ю.С. Визначення допустимих рівнів завад в енергетично-інформаційних мережах / Ю.С. Петергеря, Ю.В. Хохлов, О.В. Невмержицький // Технічна електродинаміка. Темат. вип. “Проблеми сучасної електротехніки”. - Ч.1. – 2010. – С.57-60.
13. Петергеря Ю.С. Реалізація ефективного керування споживанням електричної енергії в локальних об’єктах (за матеріалами наукової праці «Теорія та засоби побудови енергоефективних систем керування електроживленням локальних об’єктів»)/ Ю.С. Петергеря, Т.А. Хижняк, І.В. Блінов, В.В. Чопик // Технічна електродинаміка. Темат. вип. „Силова електроніка та енергоефективність”. - Ч.1. – 2010. - С.116-120.
14. Петергеря Ю.С. Основні аспекти побудови та функціонування енергоефективних систем керування локальних об’єктів (за матеріалами наукової праці «Теорія та засоби побудови енергоефективних систем керування

електроживленням локальних об’єктів») / Ю.С. Петергеря, Т.А. Хижняк, І.В. Блінов, В.В. Чопик // Праці ІЕД НАНУ. – 2010. – С.226-230.
15. J. Petergerya. Determination of Acceptable Levels of Noise in Power-line Communications / Petergerya Julia, Khokhlov Yuriy, Nevmerzhytskyi Oleg // 9th International Symposium on EMC. – 2010. – Wroclaw. – Poland. - P.800-803.
16. Терещенко Т.О. Економічний аспект споживання електроенергії в енергетичній системі мікрогрід / Т.О. Терещенко, Є.С. Пічкальов, Ю.С Ямненко // Електроніка та зв’язок. Темат. вип. “Електроніка та нанотехнології”. - № 4. – 2011. – С.109-112.
17. **Марчук Д.О. (студент).** Контурний аналіз зображень на базі функцій Хартлі / Д.О. Марчук, Ю.С. Ямненко, Т.О. Терещенко // Технічна електродинаміка. Темат. вип. „Силова електроніка та енергоефективність”, ч.2. – 2011. – С.158-163.
18. Терещенко Т.О. Применение обобщенного спектральнрого преобразования в ориентированном базисе в системах CDMA / Т.О. Терещенко, Д.В. Лазарєв // Електроніка та зв’язок. Темат. вип. “Електроніка та нанотехнології”. - № 4. – 2011. – С.79-82.
19. **Ievgenii Tsokalo (студент),** Yamnenko Yulia, and Stanislav Mudriievskyi. Backoff Algorithms Performance in Burst-Like Traffic // EUNICE 2011. – Workshop on "Energy-Aware Communications". - 5-7 September 2011. – Dresden, Germany. - P.54-64.

12. Фото / схема, слайди презентації розробки в електронному вигляді (рекламного характеру).

Розроблений та виготовлений макет тестової плати для порівняння запропонованих і декількох типових систем захисту. серед яких:

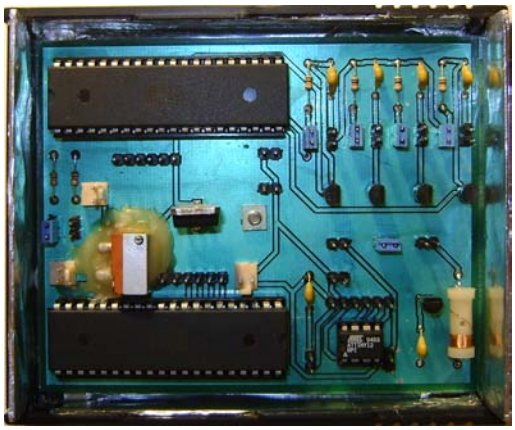

Рис. 1

- застосування вхідного фільтруючого конденсатора;
- застосування фільтрів зі змінними параметрами;
- використання стабілізатора напруги;
- система захисту на основі блоку ключів;
- система захисту на основі змінного конденсатора;
- програмна система захисту з маніпуляції внутрішніми ресурсами мікроконтролера.

Зовнішній вигляд макету наведено на рис. 1.